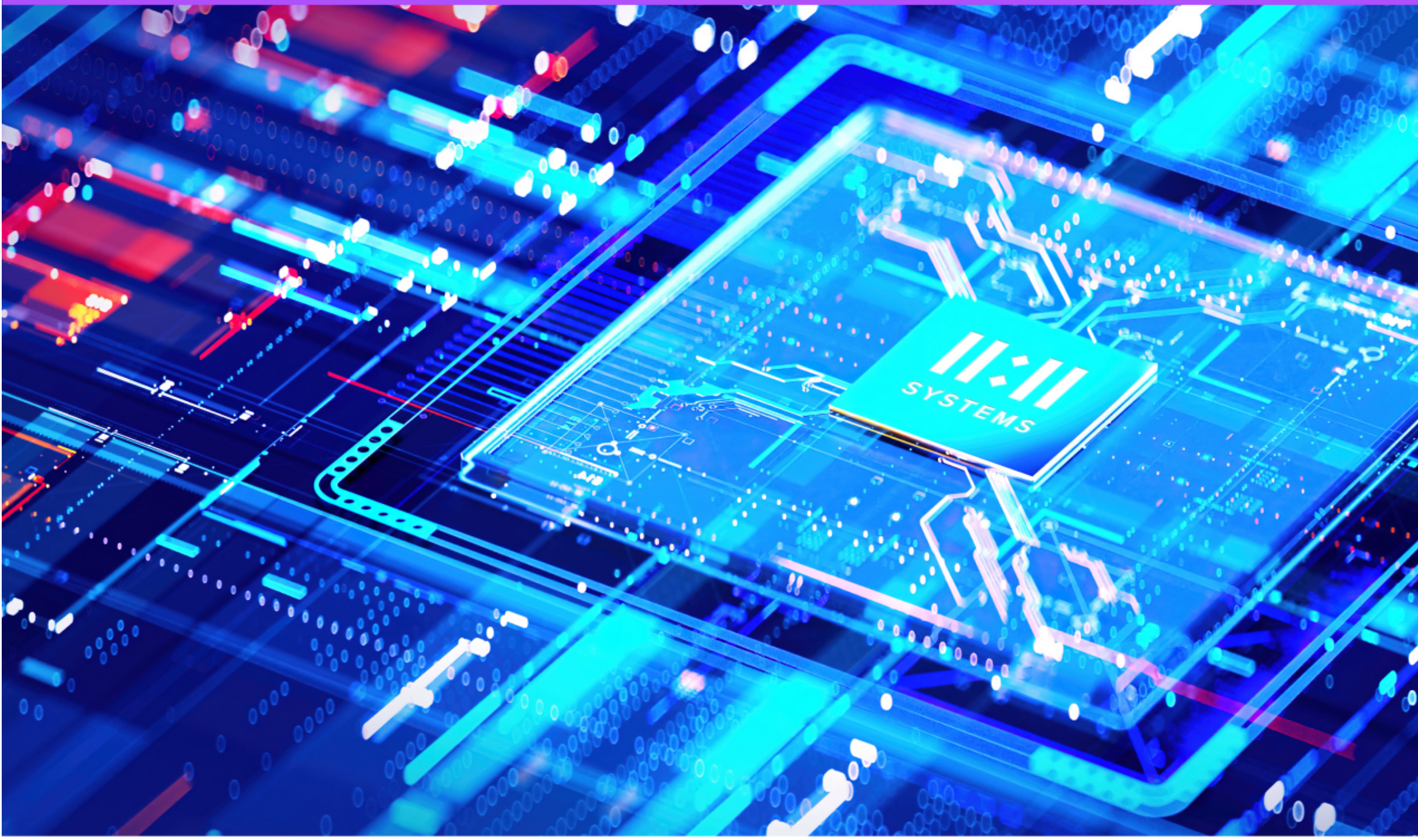
11:11 SYSTEMS

MANAGED PUBLIC CLOUD

SERVICES GUIDE



December 6, 2024

THE RESILIENT CLOUD PLATFORM

Table of Contents

Document Versioning

Version	Version Date	Comments
1.0	10/14/2024	Initial Version Release for 11:11 Systems Gen-2.0 Managed Public Cloud Services
1.1	12/6/2024	Minor Version Updates

Acronym Key

Acronym	Expanded Term
AoC	Attestation of Compliance
APM	Application performance monitoring
CDR	Customer design requirements
CSM	Customer Service Manager
CVE	Common vulnerability and exposures
DRaaS	Disaster recovery as a service
IaC	Infrastructure as code
IDS	Intrusion detection services
IPS	Intrusion prevention services
ITIL	Information Technology Infrastructure Library
PCI DSS	Payment Card Industry Data Security Standard
RCA	Root cause analysis
SLA	Service-level agreement
SOC	Security Operation Center
WAF	Web application firewall

Disclaimer

THIS INFORMATION DOES NOT CONSTITUE A FORMAL CONTRACT AND IS SOLELY AN INDICATIVE AND UNQUALIFIED STATEMENT OF SERVICES NOT CAPABLE OF ACCEPTANCE.

Accuracy: 11:11 Systems does not warrant the completeness or accuracy of the information contained herein and shall not be responsible for technical or editorial errors or omissions. Other than as stated elsewhere in this document, 11:11 Systems hereby excludes any express or implied warranties that may be contained in this document and further disclaims all liabilities which may arise due to, and/or as a consequence of, reliance on the information contained herein.

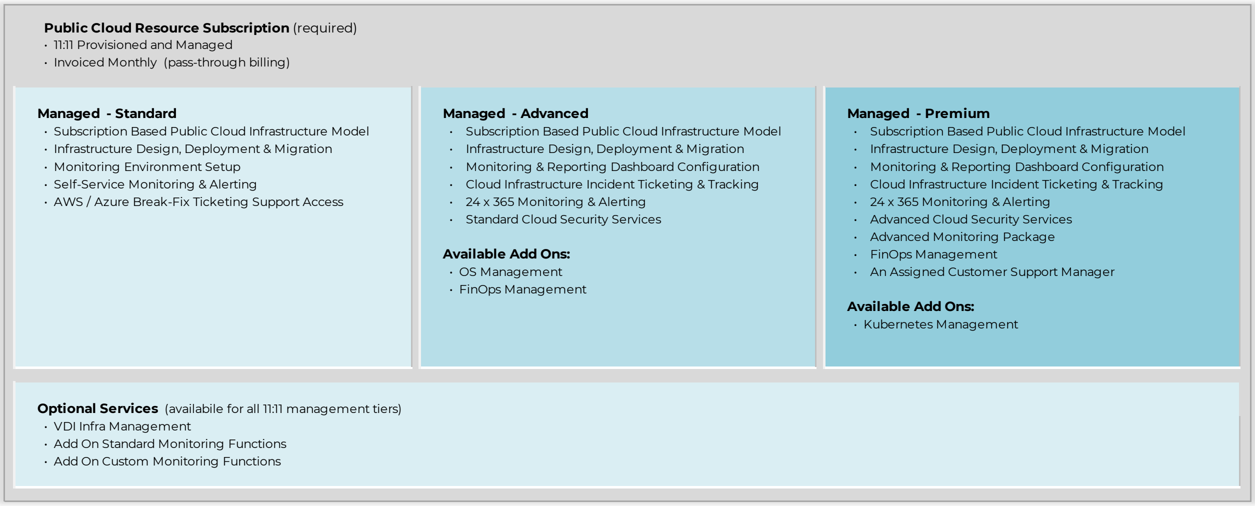
Copyright: Copyright in this document is vested in and shall remain with 11:11 Systems. No part may be reproduced or used except for the purpose for which it is supplied or as authorized by contract or other written permission. The copyright and foregoing restriction on reproduction and use extend to all media in which the information may be embodied.

1. Services Overview

Service Features and Structure

11:11 Systems uses a modern service provider model in its approach to provisioning and management services for Amazon Web Services (AWS) and Microsoft Azure. While all available service levels provide Public Cloud infrastructure design, provisioning, monitoring and break fix call access via the provider support teams.

11:11 Systems offers a wide range of cloud management tiers and options. This provides you with the flexibility to deploy the cloud operations support model that best aligns with your organization's desired level of ownership for infrastructure performance, availability and security, while optimizing team contributions, business outcomes and value. The available cloud management options are summarized below, and further described later in this document.



Public Cloud Resource Subscription (required)
- 11:11 Provisioned and Managed
- Invoiced Monthly (pass-through billing)

Managed - Standard
- Subscription Based Public Cloud Infrastructure Model
- Infrastructure Design, Deployment & Migration
- Monitoring Environment Setup
- Self-Service Monitoring & Alerting
- AWS / Azure Break-Fix Ticketing Support Access

Managed - Advanced
- Subscription Based Public Cloud Infrastructure Model
- Infrastructure Design, Deployment & Migration
- Monitoring & Reporting Dashboard Configuration
- Cloud Infrastructure Incident Ticketing & Tracking
- 24 x 365 Monitoring & Alerting
- Standard Cloud Security Services

Available Add Ons:
- OS Management
- FinOps Management

Managed - Premium
- Subscription Based Public Cloud Infrastructure Model
- Infrastructure Design, Deployment & Migration
- Monitoring & Reporting Dashboard Configuration
- Cloud Infrastructure Incident Ticketing & Tracking
- 24 x 365 Monitoring & Alerting
- Advanced Cloud Security Services
- Advanced Monitoring Package
- FinOps Management
- An Assigned Customer Support Manager

Available Add Ons:
- Kubernetes Management

Optional Services (availabile for all 11:11 management tiers)
- VDI Infra Management
- Add On Standard Monitoring Functions
- Add On Custom Monitoring Functions

Figure 1. 11:11 Systems - Public Cloud Management Options

11:11 Systems management tiers can be mixed for a single company or company organization by executing separate contract schedules. These would be deployed within a single master account with individual sub-accounts and resource pools. These can also be configured with individual period start and end dates.

Service Geographic Availability

Current geographic availability for both AWS and Azure Public Cloud within the 11:11 Systems management framework is below. All include multiple availability zones.:

AWS Data Centers (primary / backup)	**Azure Data Centers** (primary / backup)
US, North Virginia / Ohio or Oregon	**US East, Virginia** / US Central or US West
US, Ohio / North Virginia or Oregon	**US Central, Iowa** / US East or US West
US, Oregon / North Virginia or Ohio	**US West, Oregon** / US East or US Central
Canada, Central / Canada Vancouver	**Canada East, Toronto** / Canada Central
Canada, Vancouver / Canada Central	**Canada Central, Quebec** / Canada East
UK, London / In Region AZ Only	**UK South, London** / UK West
France, Paris / In Region AZ Only	**UK West, Cardiff** / UK South

Please reach out to your 11:11 sales representative or navigate to our website at 1111systems.com for assistance if you don't see a specific AWS or Azure location listed.

Cloud Adoption Framework

The cloud adoption framework that 11:11 Systems employs is shown in the diagram below. This approach allows customers to execute cloud adoption in an incremental fashion where needed. This can be driven by fixed cloud migration timelines, anticipated rates of resources consumption over time, organizational risk management associated with change and many other factors. This approach provides initial deployment flexibility as well as a continuous service improvement methodology for the life of the agreement via iteration of core processes.

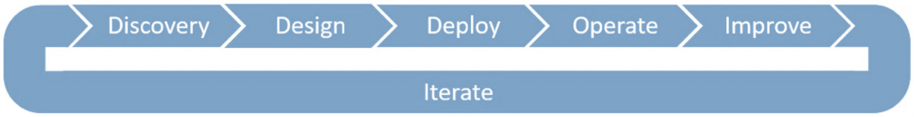


Figure 2. Cloud Adoption Framework's Iterative Approach

Following an initial discovery exercise and definition of requirements, 11:11 Systems will develop and share an architecture design based on the well architected framework guidelines supplied by the public cloud providers and 11:11 Systems' own policies. Upon design acceptance, the customer installations begin. The 11:11 Systems team uses industry-standard infrastructure as code (IaC) tools to deploy all services. The team releases resources to customers throughout the implementation process, which means customers can begin their implementation process sooner.

Following implementation and depending on the selected management support tier, the focus turns to continued improvement. Using the data provided by our comprehensive toolset, the team identifies and recommends opportunities to optimize and implement these improvements. This approach then can be repeated for additional workloads, both new and existing, as customers continue to move to cloud-based IT operations. This improvement process also can be applied during an application lifecycle, when decisions on its future state are being made. For example, when major releases are required, a customer may benefit from a cloud native design such as serverless architecture or "containerized" workloads. 11:11 Systems' certified cloud specialists are positioned to advise as those strategies develop and assist when they are implemented.

11:11 Systems brings a wealth of experience with running and supporting secure cloud workloads, and we provide best-of-breed monitoring and reporting services within the scope of all management support tiers. This enables customers to adopt the monitoring and reporting procedures that are designed to work with the public cloud without the "heavy lifting" normally required to investigate, rationalize and deploy these complex monitoring and reporting systems.

General Service Provider Relationships

11:11 Managed Cloud Services for AWS and Azure are structured against an underlying subscription with the individual Cloud provider under their master terms and conditions, which become part of the customers services agreement with 11:11: systems. The Public Cloud Infrastructure resource requirements and direct costs are estimated during the initial design and discover phases based on a customers preferred Public Cloud provider, with these resources and associated pass-through costs becoming the basis for the managed services agreement with 11:11 Systems.

Services Deployment and Billing Structures

Once the 11:11 Systems Managed Public Cloud Services contract is executed, 11:11 Systems creates and configures the AWS or Azure resources as per the agreed-upon design. Usage will commence from the time that the account is created along with the first resources, as both AWS and Azure public cloud infrastructure services utilize real-time consumption-based billing. It should be noted however that AWS and Azure resources are billable upon physical deployment, even if not fully utilized.

Upon services deployment, each customer will be provided with roles-based user access, which is established against a predetermined list of roles and responsibilities. All 11:11 Systems management tiers include access to the cloud provider's break fix resources for the deployed infrastructure. These cloud provider resources are initially accessed via the 11:11 Systems call management system with levels of ongoing cloud provider engagement and ownership through to closure being dependent upon the customer's contracted 11:11 Systems management tier.

Monthly AWS and Azure pass-through billing will vary up or down depending on consumption, including variable elements such as backup storage occupancy and network data or access fees. 11:11 Systems management fees are tied in part to all AWS or Azure pass-through fees that are under 11:11 Systems management, with these management fees varying up or down in a linear manner with respect to the associated pass-through fees for any given period.

Depending on the specific services contracted, monthly customer invoicing from 11:11 Systems is generally a combination of some advanced billing and some in arrears billing, with the associated details provided in the invoice. Customers can still take advantage of available AWS and Microsoft Azure programs for reserving infrastructure resources at discounted rates for a committed period of use, and these are then incorporated into the 11:11 Systems agreement.

Customer will be required to acknowledge within the Order that all subscriptions entered into constitutes a binding commitment for any fixed periods, including those associated with minimum term commitments that could exceed the term of the initial 11:11 Systems order, and that they will continue to be responsible for these fees until any such commitments have been fully met.

11:11 Systems will provide the following minimum services in connection with the virtual infrastructure services hosted by AWS or Microsoft Azure and managed by 11:11 Systems:

- Creation and configuration of AWS or Azure tenants and subscriptions on the customer's behalf
- Provisioned access to required tools and consoles
- Configuration, implementation, environment cloud monitoring functions
- Feature deployment as contracted and agreed-upon during design
- Infrastructure support tickets created with AWS and Microsoft Azure support
- SLA credit requests submitted on behalf of the customer and credit applied to the customer invoice, as appropriate

In addition to the minimum services listed above, additional features are applicable to specific management tiers, including configuration changes, patch management and installation, availability monitoring, and managed problem resolution of services hosted in AWS or Azure.

Customers are responsible for the following with the virtual infrastructure services hosted by Microsoft and managed by 11:11 Systems:

- Maintain licensing for any software not provided by 11:11 Systems
- Adhere to the applicable AWS and Microsoft terms and conditions
- Maintain passwords in a secure manner
- Respond to 11:11 Systems requests in a timely manner

Add-On Public Cloud Infrastructure Resources

Customers may request additional AWS or Azure resources that 11:11 Systems will configure on their behalf. These resources then will generate additional infrastructure pass-through billing, as well as the associated 11:11 Systems management billing. If a customer requests the removal of infrastructure resources, the usage-based charges will be reduced accordingly, subject to any reserved AWS or Azure resources that have a minimum commit term and associated fee commitments.

Project Work

11:11 Systems can also provide project services for work that falls outside of the scope of the contracted services. The associated Scope of Work and payment schedules for this category of project work is documented in the statement of work that accompanies the order.

Service Credits

Service-level agreements (SLAs) are provided by both AWS and Microsoft (Azure) for certain outages related to the physical infrastructure that they provide, and wherever possible, 11:11 Systems configures the customer infrastructure to the requirements that qualify for these SLAs. In the event of a breach, 11:11 Systems will pursue SLA credits with AWS or Microsoft on the customer's behalf and subsequent credits, where granted, will be applied to the following month's invoice.

Service Termination

If a customer requests to terminate their environment, 11:11 Systems will work with the customer to determine the best course of action for any resources. This may involve transitioning to a retail AWS or Azure offering, another partner's environment or may involve destroying all resources. The customer will continue to be billed for all resources until such time as 11:11 Systems is no longer billed for them by AWS or Microsoft.

Monitoring and management tools used to deliver the Managed Azure service will be disabled at service termination. Any agents or drivers installed onto customer resources will have to be removed manually. Any administrative passwords, keys, secrets, etc. will be securely transferred at this time.

2. Management Services Detail

Support Resources and Call Handling

The 11:11 Systems Managed Public Cloud support team consists in part of DevOps cross-functional 11:11 Systems associates who are focused specifically on AWS and Azure public cloud customers. This team is responsible for all Advanced and Premium tier customer incident responses, diagnosis and resolution, with the exception being any hardware infrastructure issues supported directly by the individual cloud providers (applies to all management tiers).

11:11 Systems support teams are also responsible for customer-requested change implementations and utilize ISO standardized methods and procedures for the efficient and prompt handling of all change requests. The team works to ensure that all change requests are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

Service Level Commitments

11:11 SLAs can be found here: https://www.1111systems.com/legal/sla

SLAs for AWS and Azure infrastructure services are provided by these respective providers as part of their subscription services agreements.

Network Connectivity and Customer Access

Managed Azure services provide access to portals that are important for customers to gain insight into their infrastructure, monitoring and cost/billing. Customers also get access to the 11:11 customer support portal for raising support ticket for requests, changes and incidents.

Services related portals provided to customers as part of 11:11 Managed Cloud for Azure include:

- A Billing Portal
- A Monitoring & Observability Portal
- A Managed Azure Portal for Ticketing and Support Communications

Cloud and Operational Security

11:11 Systems operates within a structured security framework, aligning to a diverse range of compliance requirements that enforce intrinsic security. Customers’ benefit from our ability to extend this security framework to encompass the security features and services available from AWS and Azure in meeting our customers’ individual compliance and security needs.

These extended public cloud security features include:

AWS Security Portfolio	Azure Security Portfolio
PCI/DSS Conformance Pack	Azure Policy Automation
Amazon Guard Duty (continuous threat monitoring)	Azure Network Security Groups
Amazon Inspector (security assessments)	Azure Key Vault (API Keys, passwords, certificates, etc.)
Security Hub (security alert dashboard / aggregator)	Azure Firewall
Symantec Antivirus Protection for Windows & Linux	Optional: Azure Application Gateway, Azure Advanced Threat Protection, Centralized Log Management SIEM
In Transit Network Data Security	
AWS Firewall	

Data Protection

11:11 Systems provides backup services to the 11:11 Managed Cloud for customers who take advantage of the Azure native Recovery Services Vault service for backup.

Configurable backup policy parameters include:

- Weekly Retention (# of Weeks)
- Monthly Retention (# of Months)
- Yearly Retention (# of Years)
- Archive-tier support is also available for long-term retention

Environment Recoverability

11:11 Systems can design, build and test a recovery solution utilizing secondary site public cloud resources. Recovery services include failover and fail back, with SLA backed Recovery Time Objectives.

Available services include:

- A customized recovery plan for virtual machine and application boot order priorities
- Reporting for real-time RPO levels and resource utilization
- Recovery certificate and audience segregated reporting for auditing purposes

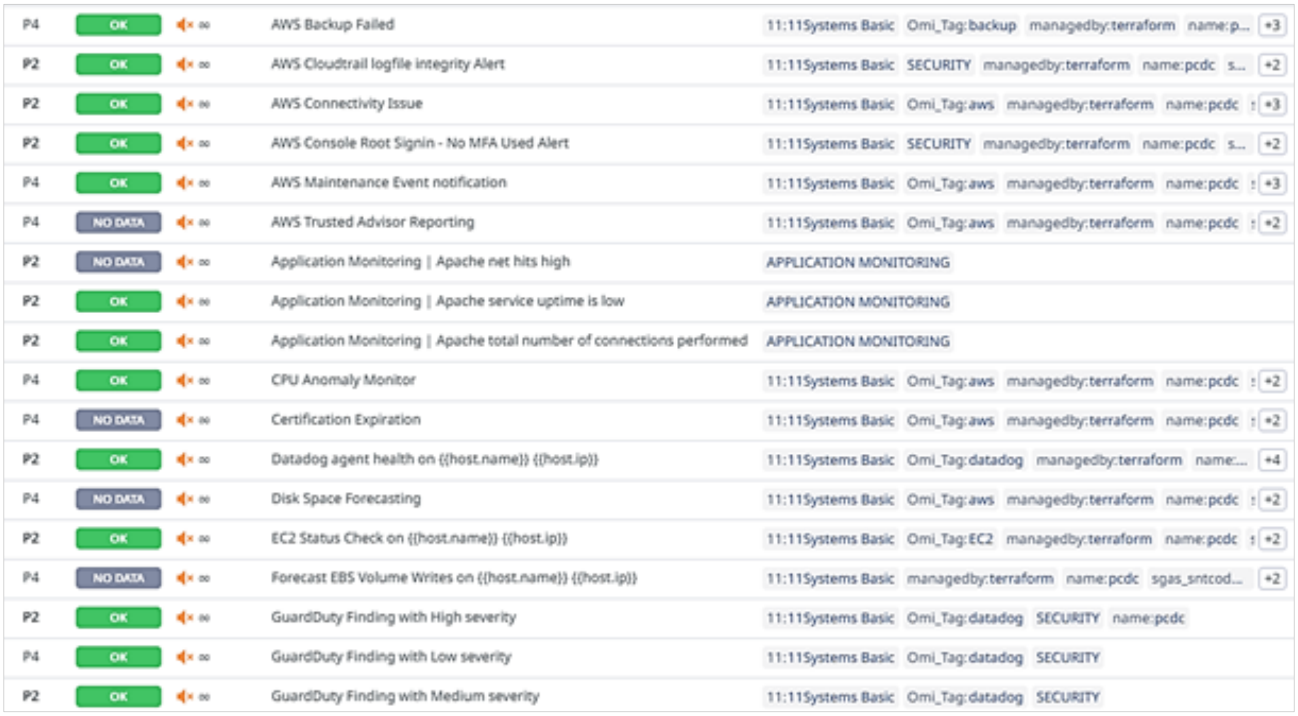
Storage Options

Resource planning during the design phases will identify the various cloud storage options available and the most appropriate performance and capacity-based choices for the initial resource selections.

Monitoring

Managed Cloud for AWS & Azure utilized a SaaS based monitoring and observability tool. This tooling platform enhances visibility into your environment and aids in maintaining high-performance systems, while reducing downtime and operational overhead. Features Include:

- **Unified Monitoring:** Consolidates metrics, traces, and logs in one platform, providing a comprehensive view of your systems and applications.
- **Real-time Visibility**: We offer real-time monitoring and alerts, helping you quickly identify and resolve issues before they impact users.
- **Integrations:** We support a wide range of integrations with various technologies, tools, and services, allowing you to monitor diverse environments easily.
- **User-friendly Interface:** The intuitive dashboard and visualizations make it easier for customers to understand data and act on insights.



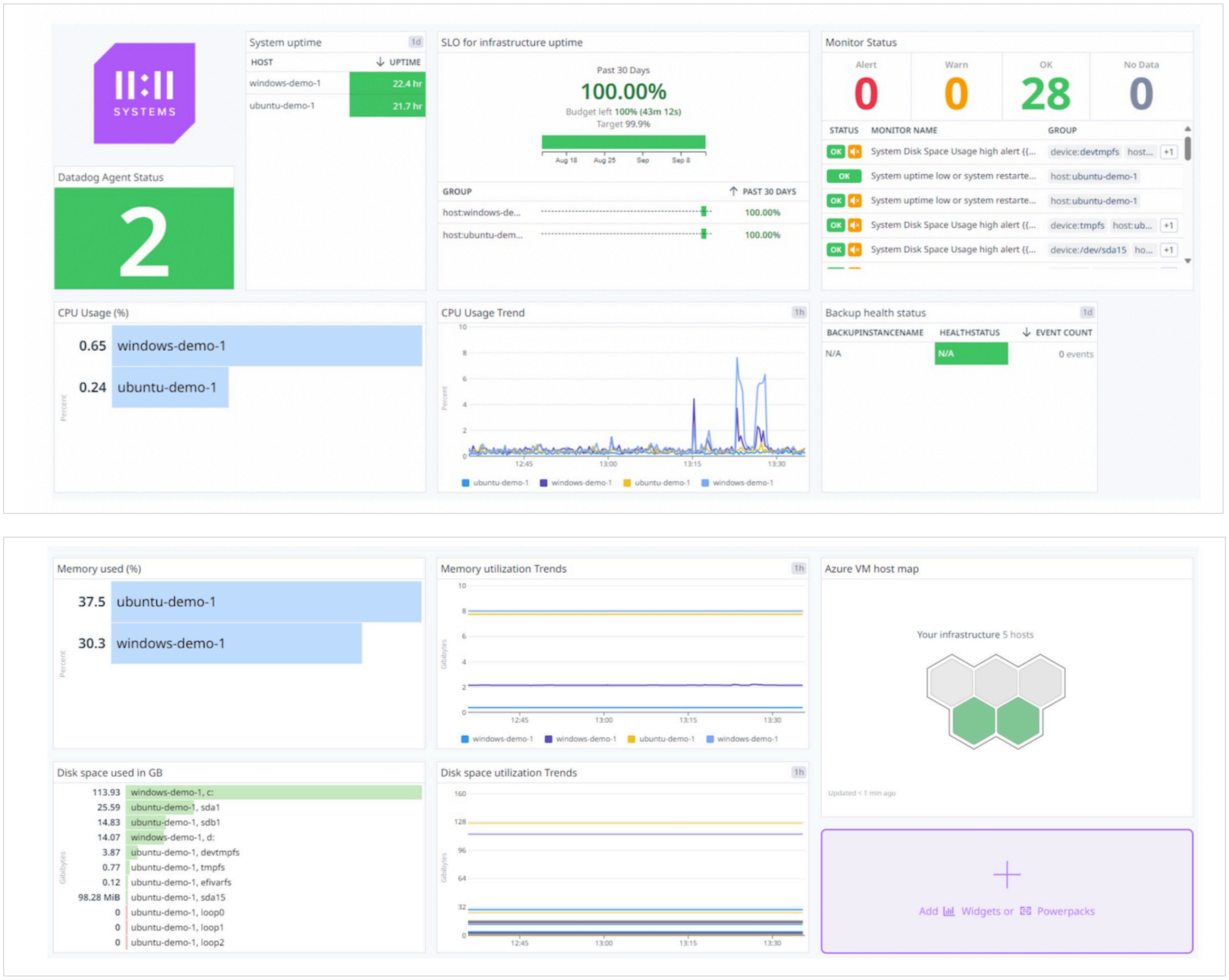
P4	OK	AWS Backup Failed	11:11Systems Basic Omi_Tag:backup managedby:terraform name:p... +3
P2	OK	AWS Cloudtrail logfile integrity Alert	11:11Systems Basic SECURITY managedby:terraform name:pcdc s... +2
P2	OK	AWS Connectivity Issue	11:11Systems Basic Omi_Tag:aws managedby:terraform name:pcdc : +3
P2	OK	AWS Console Root Signin - No MFA Used Alert	11:11Systems Basic SECURITY managedby:terraform name:pcdc s... +2
P4	OK	AWS Maintenance Event notification	11:11Systems Basic Omi_Tag:aws managedby:terraform name:pcdc : +3
P4	NO DATA	AWS Trusted Advisor Reporting	11:11Systems Basic Omi_Tag:aws managedby:terraform name:pcdc : +2
P2	NO DATA	Application Monitoring | Apache net hits high	APPLICATION MONITORING
P2	OK	Application Monitoring | Apache service uptime is low	APPLICATION MONITORING
P2	OK	Application Monitoring | Apache total number of connections performed	APPLICATION MONITORING
P4	OK	CPU Anomaly Monitor	11:11Systems Basic Omi_Tag:aws managedby:terraform name:pcdc : +2
P4	NO DATA	Certification Expiration	11:11Systems Basic Omi_Tag:aws managedby:terraform name:pcdc : +2
P2	OK	Datadog agent health on {{host.name}} {{host.ip}}	11:11Systems Basic Omi_Tag:datadog managedby:terraform name:... +4
P4	NO DATA	Disk Space Forecasting	11:11Systems Basic Omi_Tag:aws managedby:terraform name:pcdc : +2
P2	OK	EC2 Status Check on {{host.name}} {{host.ip}}	11:11Systems Basic Omi_Tag:EC2 managedby:terraform name:pcdc : +2
P4	NO DATA	Forecast EBS Volume Writes on {{host.name}} {{host.ip}}	11:11Systems Basic managedby:terraform name:pcdc sgas_sntcod... +2
P2	OK	GuardDuty Finding with High severity	11:11Systems Basic Omi_Tag:datadog SECURITY name:pcdc
P4	OK	GuardDuty Finding with Low severity	11:11Systems Basic Omi_Tag:datadog SECURITY
P2	OK	GuardDuty Finding with Medium severity	11:11Systems Basic Omi_Tag:datadog SECURITY

Figure 3. Sample Monitors (AWS)

Reporting

11:11 Systems provides real-time reporting dashboards for Managed Public Cloud services and the applications running on those services. For ease of access, we publish dashboards with preselected reports and customers can view additional data using the “drill-down” capabilities of our monitoring systems. Note that custom static or dynamic monitoring elements are orderable as an option for all management tiers. Customers are also provided with direct access to cost and compliance reports, with specific reporting elements, level of detail and consultative inputs dependent on the contracted management tier and add-on reporting options.

The sample monthly dashboard views shown in the two following figures are available for all management tiers, and provide a summary of key data points, including host and infrastructure availability, alert data and CPU utilization, etc. Detail drilldowns are available as well.



Datadog Agent Status
2

System uptime 1d

HOST	↓ UPTIME
windows-demo-1	22.4 hr
ubuntu-demo-1	21.7 hr

SLO for infrastructure uptime
Past 30 Days
100.00%
Budget left 100% (43m 12s)
Target 99.9%

GROUP	↑ PAST 30 DAYS
host:windows-de...	100.00%
host:ubuntu-dem...	100.00%

Monitor Status

Alert	Warn	OK	No Data
0	0	28	0

STATUS	MONITOR NAME	GROUP
OK	System Disk Space Usage high alert {{...	device:devtmpfs host... +1
OK	System uptime low or system restarte...	host:ubuntu-demo-1
OK	System uptime low or system restarte...	host:ubuntu-demo-1
OK	System Disk Space Usage high alert {{...	device:tmpfs host:ub... +1
OK	System Disk Space Usage high alert {{...	device:/dev/sda15 ho... +1

CPU Usage (%)

0.65	windows-demo-1
0.24	ubuntu-demo-1

Backup health status 1d

BACKUPINSTANCENAME	HEALTHSTATUS	↓ EVENT COUNT
N/A	N/A	0 events

Memory used (%)

37.5	ubuntu-demo-1
30.3	windows-demo-1

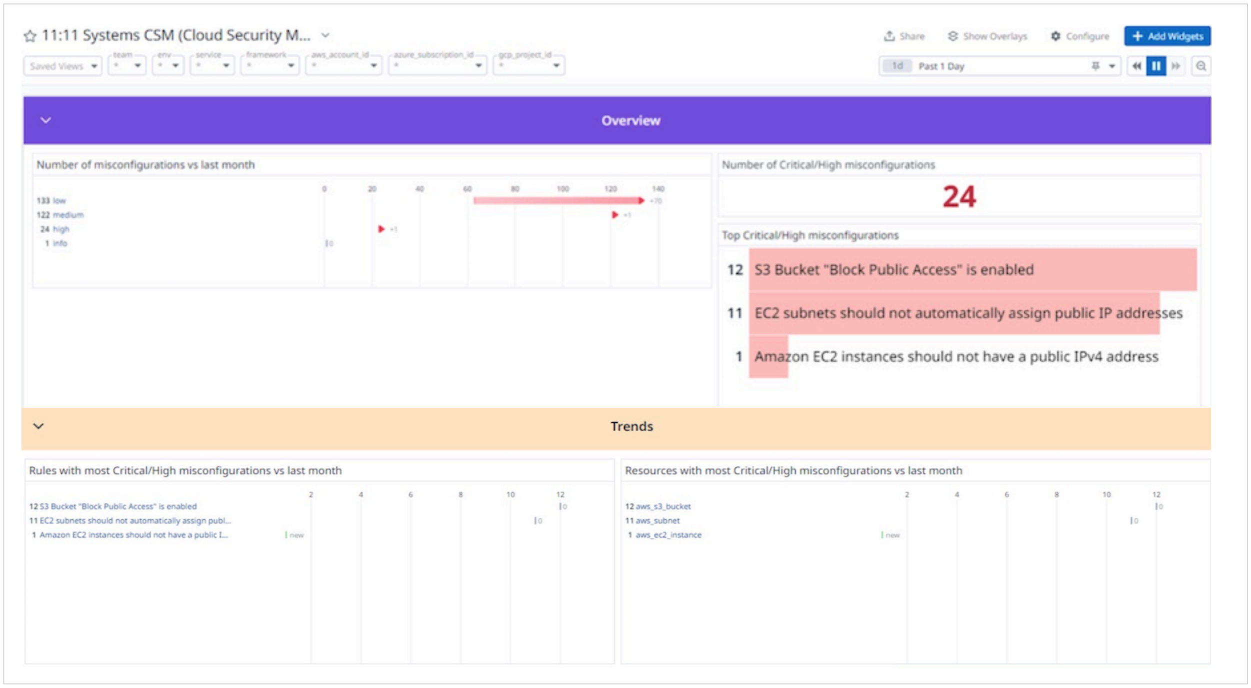
Disk space used in GB

113.93	windows-demo-1, c:
25.59	ubuntu-demo-1, sda1
14.83	ubuntu-demo-1, sdb1
14.07	windows-demo-1, d:
3.87	ubuntu-demo-1, devtmpfs
0.77	ubuntu-demo-1, tmpfs
0.12	ubuntu-demo-1, efivarfs
98.28 MiB	ubuntu-demo-1, sda15
0	ubuntu-demo-1, loop0
0	ubuntu-demo-1, loop1
0	ubuntu-demo-1, loop2

Azure VM host map
Your infrastructure 5 hosts
Updated < 1 min ago

Figure 4. Monthly Dashboard Views A and B

The sample Cloud Security view below is part of the Cloud Security feature set in the Advanced and Premium management tiers.


11:11 Systems CSM (Cloud Security M...
Share
Show Overlays
Configure
Add Widgets
Saved Views
team
env
service
framework
aws_account_id
azure_subscription_id
gcp_project_id
1d Past 1 Day
Overview
Number of misconfigurations vs last month
0 20 40 60 80 100 120 140
133 low
122 medium
24 high
1 info
+70
+1
+1
0
Number of Critical/High misconfigurations
24
Top Critical/High misconfigurations
Trends
Rules with most Critical/High misconfigurations vs last month
Resources with most Critical/High misconfigurations vs last month
2 4 6 8 10 12
new
0

Top Critical/High misconfigurations

12	S3 Bucket "Block Public Access" is enabled
11	EC2 subnets should not automatically assign public IP addresses
1	Amazon EC2 instances should not have a public IPv4 address

Rules with most Critical/High misconfigurations vs last month

12 S3 Bucket "Block Public Access" is enabled
11 EC2 subnets should not automatically assign publ...
1 Amazon EC2 instances should not have a public I...

Resources with most Critical/High misconfigurations vs last month

12 aws_s3_bucket
11 aws_subnet
1 aws_ec2_instance

Figure 5. Security Monitoring and Reporting

Application monitors such as the Apache sample below can be created as well.

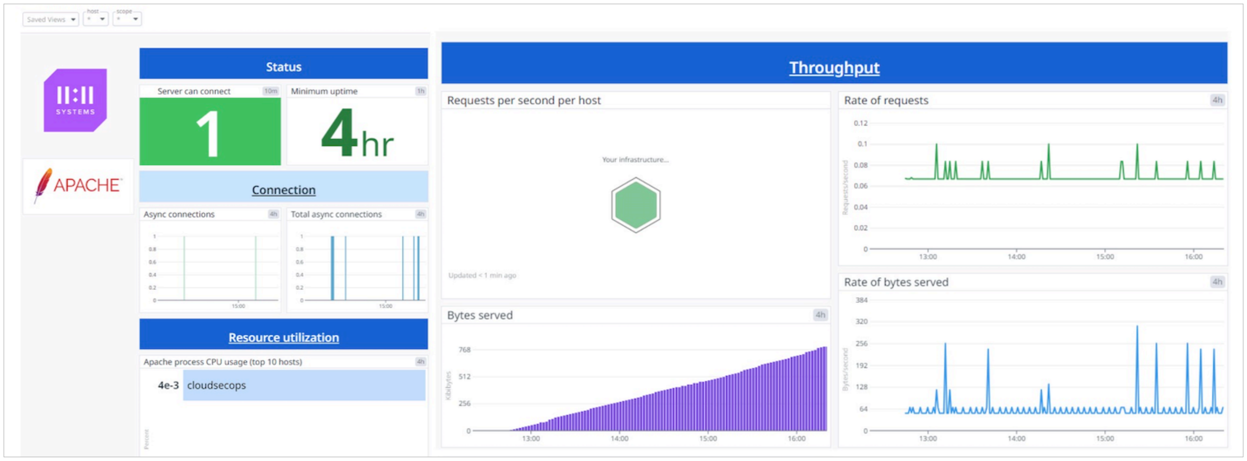


Figure 6. Application Performance Monitoring and Reporting

3. Operations Services Roles and Responsibilities

The following table outlines 11:11 Systems and customer responsibilities using a RACI model.

R	Responsible: Do the task
A	Accountable: Approve the task
C	Consulted: Input provided to the task
I	Informed: Notified on task progress or completion

Managed Public Cloud – AWS & Azure RACI Table

TASK or FUNCTION	11:11 Systems	Customer
Pre-Sales		
Full and accurate disclosure of all functional and non-functional requirements along with drivers and desired business outcomes (to include capacity, performance, security, compliance, regulatory, availability, backup & DR and scalability)	I	A, R
Collaborative high-level solution design & configuration specification	A, R	C, I
Design Review (high level solution design and how they align with desired business outcomes)	A, R	C, I
Create pre-sales design and proposal documentation	A, R	C, I
Final proposal to customer	A, R	I
Contract signature	A, C, I	R
Project Kickoff		
Sales turnover to Managed Public Cloud team	A, R	
Internal project kickoff	A, R, C	
Project kickoff - customer	A, R, C, I	R
Project Planning		
Detailed design phase (low level design documentation and approval)	A, R	C, I
Project scope definition	A, R, C, I	C
Project schedule	A, R, C, I	C, I
Verify solution and timeline requirements	A, R	I
Project Execution		
Customer Org & Account set up	A, R	I
Managed services within VPC / Virtual Network	A, R	I
Capture desired patch groups, baselines and maintenance windows as required for OS patch management [1]	A, R	I
Determine appropriate monitoring coverage and alerting thresholds along with related notification and response procedures [1]	A, R	I
Deploy Customer Architecture as per the solution design following IaC including peer review	A, R	I

▸ ***Project Execution - Continued***		
Configure VPC / Virtual Network connectivity according to design	A, R	I
Enable OS management [1]	A, R	I
Configure cloud platform backup where applicable	A, R	I
Test HA configuration where applicable	A, R	I
Configure Cloudcheckr access for configuration reporting	A, R	I
Optional: Enhanced Monitoring Setup [1]	A, R	I
Optional: Enhanced Security Services [1]	A, R	I
Managed Environment - Engineering Turn Over		
Confirmation of Management	A, R	I
Confirmation of Orchestration	A, R	I
Confirmation of customer connectivity (e.g. IPsec VPN, jump Host, Direct Connect/ExpressRoute, VPN Site-to-Site)	A, C	R, I
Notify Transition PM that all configuration complete	A, R	I
Managed Services Implementation and configuration complete	A, R	I
Test and Acceptance		
Validation tasks completed	A, R, C	I
Confirm customer access to service management portals (support and ticketing)	A, R	C
Confirm customer access to the monitoring environment	A, R	C
Cloudcheckr registrations sent, and User Guide access provided to customer.	A, R	C, I
Sign-off Monitoring scope	C, I	A, R
Sign-off OS patching configuration [1]	C, I	A, R
Review and validation of environment (e.g. Inspector, GuardDuty, Trusted Advisor, CUR)	A, R	C
Service Transition environment turn over	A, R, C, I	I
Service Delivery Validation		
PM/SME validation document complete	A, R, C, I	I
Hand off to customer	A, R, C, I	I
Install and configure applications	I	A, R
Enable application monitoring integration where applicable	A, R	C, I
Application configuration to support monitoring integration where applicable	C, I	A, R
Validate customer access to environment and operational tooling	A, R	I
Onboarding project closure	A, R	I

Monitoring and Response		
Monitor availability of Cloud resources required to deliver customer solution	R, A	I
Monitor Cloud platform health notifications for outages or notice of upcoming changes that will impact availability or operation of customer solution [1]	R, A	I
Acknowledge, investigate and notify customer of events [1]	R, A	C, I
Execute change requests and work to resolve incidents as described in the service description	R, A	C, I
Provide details/runbooks of all client-executed startup, response, failover & recovery procedures [1]	I	R, A
Provide up to date contact information for change authorization, alerting and escalation	I	R, A
Notify 11:11 Systems of any activities that may impact the availability of the application or monitored services.	C, I	R, A
Security		
Configuration of public cloud environment in alignment with security best practices	R, A	C, I,
Encryption of data in transit subject to workload requirements	R, A	C, I,
Encryption of data at rest subject to workload requirements	R, A	C, I,
Network and firewall configuration	R, A	C, I,
Secure user access management in line with best practices and adhering to the principle of least privilege	R, A	C, I,
Management of HTTPS certificates (platform provided)	R, A	C, I,
Management of HTTPS certificates (customer provided)	C, I	R, A
Propose and support the use of platform security services relevant to the workload	R, A	C, I,
Propose and support the use of 3rd party security services as required to meet the customer requirements	R, A	C, I,
Security of applications, workloads and libraries	I	R, A
Availability, Backup/Restore and Disaster Recovery		
Architect for maximum availability in compliance with best practice within the constraints of the customer design and budget	R, A	C, I
Configure the cloud platform backup service as required to meet the customers' data protection needs up to the limit of the native capabilities (e.g. snapshot frequency)	R, A	C, I
Facilitate the restoration of volume snapshots as required to restore service or to allow the client to perform file-level recovery from the snapshot	R, A	C, I
File level recovery from volume snapshot	C, I	A, R
Propose and deliver additional DR services as required to meet the customer requirement	R, A	C

OS Management		
Configuration and maintenance of AV configuration [1]	R, A	C, I
Configuration of platform automation for OS patch management in accordance with agreed baselines and schedules as per design [1]	R, A	C, I
Provide access to patch compliance reports as supported by the cloud platform [1]	R, A	I
Update and maintenance of machine images used in autoscaling launch templates [1]	C, I	R, A
Cost Management		
Provide ongoing cost-optimization recommendations [1]	R, A	I
Provide access to cost management portal & reporting	R, A	I
Configure billing alerts	R, A	C
Support		
Ongoing support and troubleshooting of Cloud solution up to the OS level [1,2]	R, A	C, I
Creation and management of support cases with the Cloud Provider	R, A	I
Conduct Monthly Service Reviews [1]	R, A	I
Conduct Quarterly Business Reviews [1]	R, A	C, I
Sharing of feedback and business updates objectives relevant to the delivered managed service [1]		R, A
Provide ongoing access to Cloud Solution architect [1]	R, A	
Provide assigned CSP, SME [1]	R, A	
Supporting and troubleshooting of customer application [1]	I	R, A
Supporting and troubleshooting of customer-managed 3rd party integration [1]	I	R, A
Submit change requests and request items in line with the timelines as described in the service guide, including adequate description and correct prioritization	I	R, A
Ensure compatibility of workloads with O/S versions and patch upgrades [1]	I	R, A
Application		
Ensure adequate license coverage for all workload components where licenses are not acquired as part of the cloud service	I	R, A
Perform all application installs, maintenance and troubleshooting	I	R, A
Assist in configuration of state/data replication as required to meet high availability or autoscaling design requirements	R	A
Configuration of application monitoring as supported by the operational toolset, including the configuration of alerting for nominated customer stakeholders	I	R, A

[1] Service feature is management tier dependent (excluded from Standard; optional for Advanced, standard for Premium)

[2] Enhanced rights where appropriate; full admin access is limited to 11:11 Systems personnel

4. Service Features and Options

Overview

The following sections describe 11:11 Systems' Cloud adoption services, as well as available post deployment Managed Cloud service features and options for AWS and Azure.

Note that the availability of some of the listed options may be limited to specific management-tiers. Please contact your 11:11 sales or support representative to inquire about any service features of interest that are listed here or are not on your current 11:11 Systems Managed Cloud contract.

Cloud Readiness Assessment

A Cloud Readiness Assessment is a project based, for fee service that can help customers who are moving a significant number of applications into the cloud, or where the migration process would involve significant transformation activity.

The Cloud Readiness Assessment's in-depth discovery and design service delivers a robust target architecture and adoption plan. Although not generally required, 11:11 Systems may require a Cloud Readiness Assessment prior to the execution of Managed Cloud Services agreement if deemed necessary. Work would be carried out via a public cloud project services engagement and defined by a statement of work.

Architecture Review

An Architecture Review ensures that any existing public cloud deployments follow best practices as described by the well-architected principles defined by the public cloud provider. This is included as a presales function for any Managed Cloud Services project involving the transition of an existing public cloud environment to 11:11 Systems management.

Migration Services

The public cloud simple migration service enables customers to quickly realize the benefit of migration by swiftly moving workloads to AWS or Azure and decommissioning legacy systems.

The simple migration service provides a customer with a low-risk, benefit-optimized transition plan to migrate their services onto the platform. With a proven methodology, tools and experience gained from prior migrations, 11:11 Systems uses a highly collaborative process that involves works closely with the customer's IT and business teams to enable a "lift and shift" approach to move Intel-based workloads into AWS or Azure. This approach enables 11:11 Systems to develop and execute a migration plan based on proven strategies that incorporate the identification of dependencies and rollback plans, and also enables testing in advance of the final migration.

A software agent is implemented to efficiently replicate an image of the machine into the chosen public cloud provider. These images are made available for testing at any time while replication continues in the background. 11:11 Systems recommends that at least one test event is performed, but a customer can elect to perform as many tests as required. This ensures that all risks are understood and managed. The service is priced based on scale and the number of migration events and migration test events.

Managed Cloud Service Tiers

11:11 Managed Cloud Services are structured against an underlying subscription with the individual Cloud provider for the cloud infrastructure portion (AWS or Azure), with an added services layer for deployment, ongoing operations and overall management. 11:11 Systems offers several management tiers and associated options that provide our customers with greater flexibility in aligning specific features to their operations requirements – which can also be modified over time or even varied by environment type (e.g. development verses production). The initially selected management tier can also be changed within the term of the contract.

Standard Services Tier

- Subscription Based Public Cloud Infrastructure Model
- Infrastructure Design, Deployment & Migration
- Environment Setup with Self-Service Monitoring & Alerting
- AWS / Azure Break-Fix Ticketing Support Access

The Standard management tier is ideal for customers that have a strong understanding of Public Cloud architecture principals as well as operations expertise. Under this management tier, 11:11 Systems provides a solid foundation for design validation and infrastructure deployment, taking advantage of 11:11 Systems deployment best practices, technical competencies and organizational depth. This can take much of the risk out of a new public cloud deployment, where unexpected infrastructure complexities and technical configuration challenges can arise.

11:11 Systems provides a best-in-class monitoring platform which is turned over for self-service use upon completion of the new cloud deployment. Under the Standard management tier, day-to-day operations support, monitoring incidents and issues relating to the public cloud infrastructure are owned by the customer team. 11:11 Systems will assist during Normal Business Hours with environment infrastructure adds/deletes and any issues related to the monitoring function, as well as facilitating Normal Business Hours access to AWS / Azure break-fix ticketing and support.

Advanced Services Tier

- Subscription Based Public Cloud Infrastructure Model
- Infrastructure Design, Deployment & Migration
- Monitoring & Reporting Dashboard Configuration
- Cloud Infrastructure Incident Ticketing & Tracking
- 24 x 365 Monitoring & Alerting
- Standard Cloud Security Services
- An Assigned Customer Support Manager
- Optional OS Management
- Optional FinOps Management

The Advanced management tier is a turn-key solution for Public Cloud design, deployment and ongoing operations. Everything from initial design recommendations to infrastructure deployment and migration is handled by an experienced team of 11:11 Systems specialists.

Once fully deployed, 11:11 Systems is heavily involved in the day-to-day support of the customer environment. This includes environment monitoring and reporting with our best-in-class monitoring platform, with 24 x 365 event capture, alerting and problem resolution. General cloud security services include the setup and management of native security monitors.

Available Options:

- The Advanced management tier can be optioned to include Operating System patching and administration. This includes all virtual machines within the managed cloud environment

- FinOps management for Cloud usage and cost optimization is also available as an option and provides analysis regarding subscription purchases, resource consumption and architectural optimization. This is performed on an annual basis, with ongoing input and guidance regarding general cloud usage efficiency.

A Customer Service Manager will be assigned to each Advanced management tier customer as a general point of contact that can assist with non-technical queries and liaise with the cloud operations teams as needed. This role is intended to ensure that each customer's support expectations are being addressed. The Customer Support Manager also meets with each customer on a regular basis to review monthly service reports on performance, resource consumption and general non-technical operational matters.

Premium Services Tier

- Subscription Based Public Cloud Infrastructure Model
- Infrastructure Design, Deployment & Migration
- Monitoring & Reporting Dashboard Configuration
- Cloud Infrastructure Incident Ticketing & Tracking
- 24 x 365 Monitoring & Alerting
- Advanced Cloud Security Services
- Advanced Monitoring Package
- FinOps Management
- An Assigned Customer Support Manager
- Optional Kubernetes Management

The Premium management tier includes all of the features of the Advanced management tier, and adds the following:

- Managed Operating System support is standard

- FinOps support is standard

- An advanced monitoring package that includes synthetic monitoring of web application transactions, real-user monitoring, process monitoring, application performance monitoring (APM), and log management

- Advanced security package network security reporting, virtual machine vulnerability scanning and general AV management.

Available Options:

- Kubernetes Management
    - Cluster Provisioning
    - Networking Setup
    - Horizontal Pod Autoscaling (HPA)
    - Cluster Autoscaler
    - Load Balancers
    - Monitoring
    - Logging
    - Alerts and Dashboards
    - Security and Compliance
        - RBAC (Role-Based Access Control
        - Secrets Management
    - Upgrades and Patches
        - Kubernetes Version Management
        - Security Patches/Updates
    - Cost Management
        - Cost Optimization
    - Tools for Kubernetes Management
        - kubectl

Optional Services – All Tiers

- VDI Infra Host Management
- Add-On Standard Monitoring Functions
- Add-On Custom Monitoring Functions

- A VDI host solution is available and can be configured as a standalone environment with any of the 11:11 Systems cloud management tiers. Please consult your 11:11 Sales representative for more information.

- In addition to the base monitoring suite, custom monitors can be added for an additional monthly fee. This includes both standard "out of the box" monitoring functions and customizable monitoring functions.

Project Services

11:11 Systems provides standalone project service to enhance your usage of public cloud. This service enables customers to order blocks of hours for project services and are generally used for activities that fall outside of the cloud management services scope or for upfront cloud readiness assessments.

Each project engagement will include a Statement of Work relative to the scope, fees and timing of the hourly engagement.